Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (Currently Amended) A method of processing a packet having a plurality of layers wherein a first layer is structured in accordance with a first protocol and a second layer is structured in accordance with a second protocol, comprising:

processing [[a]] the first layer of the packet in accordance with the first protocol and a first ~~protocol~~ security policy; and

processing [[a]] the second layer of the packet in accordance with the second protocol and a second ~~protocol~~ security policy at least partially in parallel with processing of ~~said~~ the first layer of the packet when processing of ~~said~~ the first layer[[s]] of the packet uncovers sufficient information to support security processing of ~~said~~ the second layer of the packet.

2. (Currently Amended) A method of processing a data packet having a plurality of layers according to a plurality of security policies, comprising the steps of:

(a) receiving the data packet;

(b) identifying a first security policy associated with a first layer of the data packet;

(c) processing the first layer of the data packet according to the first security policy;

(d) identifying a second security policy associated with a second layer of the data packet when information necessary for ~~said~~ the identification of the second security policy becomes available during the processing of the first layer of the data packet; and

(e) processing the second layer of the data packet according to the second security policy, wherein processing the first layer of the data packet according to the first security policy occurs at least partially concurrently with the step [[(c)]] of processing the second layer of the data packet according to the second security policy.

3. (Original) The method of claim 2, wherein said step (c) comprises decryption of data in the packet.

4. (Original) The method of claim 3, wherein said decryption is performed according to the data encryption standard (DES).

5. (Original) The method of claim 3, wherein said decryption is performed according to the triple data encryption standard (3DES).

6. (Original) The method of claim 3, wherein said decryption is performed according to the ARC4 algorithm.

7. (Original) The method of claim 2, wherein said step (e) comprises decryption of data in the packet.

8. (Original) The method of claim 7, wherein said decryption is performed according to the DES.

9. (Original) The method of claim 7, wherein said decryption is performed according to the 3DES.

10. (Original) The method of claim 7, wherein said decryption is performed according to the ARC4 standard.

11. (Original) The method of claim 2, wherein said step (e) comprises authentication of the data packet.

12. (Previously Presented) The method of claim 11, wherein said authentication comprises application of the Multilinear Modular Hashing (MMH) algorithm.

13. (Original) The method of claim 11, wherein said authentication comprises application of the Hash-based Message Authentication Code (HMAC) Secure Hash Algorithm (SHA)-1.

14. (Original) The method of claim 2, wherein said step (e) comprises re-encryption of decrypted data from the packet.

15. (Original) The method of claim 14, wherein said re-encryption comprises encryption performed according to the Advanced Encryption Standard (AES).

16. (Currently Amended) A system for processing a data packet having a plurality of layers according to a plurality of security policies, wherein the data packet comprises a first and second layer, the first layer associated with a first security policy and the second layer associated with a second security, and wherein processes that effect respective security policies for the first and second layers of the data packet can execute in parallel, the system comprising:

~~a packet identification (PID) parser that identifies the packet;~~

a ~~plurality of~~ first security processing module[[s,]] ~~each of which can~~ configured to process the first layer of the data packet according to ~~one of~~ the first security policy; and

~~policies in parallel with at least one other~~ a second security processing module processing the second layer of the data packet according to the second security policy;~~and~~

wherein the first and second security processing modules process the first and second layers of the data packet at least partially in parallel.

~~at least one feedback loop or feeding output of at least one of said security processing modules to at least one other security processing module.~~

17. (Currently Amended) The system of claim 16, wherein ~~said~~ the first security processing module[[s]] comprises a module for performing decryption according to the DES.

18. (Currently Amended) The system of claim 16, wherein ~~said~~ the first security processing module[[s]] comprises a module for performing decryption according to the 3DES.

19. (Currently Amended) The system of claim 16, wherein ~~said~~ the first security processing module[[s]] comprises a module for performing Digital Video Broadcast (DVB) descrambling.

20. (Currently Amended) The system of claim 16, wherein ~~said~~ the first security processing module[[s]] comprises a module for performing HMAC authentication.

21. (Previously Presented) The method of claim 3, wherein said decryption is performed in application layer processing.

22. (Previously Presented) The method of claim 11, wherein said authentication is performed in application layer processing.

23. (New) The system as set forth in claim 16, further comprising a packet identification (PID) parser that identifies the packet.

24. (New) The system as set forth in claim 16, further comprising at least one feedback loop or feeding output of at least one of said security processing modules to at least one other security processing module.